INSTITUTE FOR DEFENSE ANALYSES

NSD-5216

A Consistent Approach for Security Risk Assessments of Dams and Related Critical Infrastructure

J. Darrell Morgeson
Jason A. Dechant
Yev Kirpichevsky
Yazmin Seda-Sanabria, U.S. Army Corps of Engineers
Enrique E. Matheu, U.S. Department of Homeland Security

June 2014

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

NSD-5216

A Consistent Approach for Security Risk Assessments of Dams and Related Critical Infrastructure

J. Darrell Morgeson
Jason A. Dechant
Yev Kirpichevsky
Yazmin Seda-Sanabria, U.S. Army Corps of Engineers
Enrique E. Matheu, U.S. Department of Homeland Security

June 2014

A Consistent Approach for Security Risk Assessments of Dams and Related Critical Infrastructure

James D. Morgeson[1], Yazmin Seda-Sanabria[2], Yevgeniy Kirpichevsky[3], Jason A. Dechant[4], and Enrique E. Matheu[5]

[1] *Institute for Defense Analyses, Alexandria, VA 22311, USA. jmorgeso@ida.org*
[2] *Office of Homeland Security, Directorate of Civil Works, U.S. Army Corps of Engineers, Washington, DC 20314, USA. Yazmin.Seda-Sanabria@usace.army.mil*
[3] *Institute for Defense Analyses, Alexandria, VA 22311, USA. ykirpich@ida.org*
[4] *Institute for Defense Analyses, Alexandria, VA 22311, USA. jdechant@ida.org*
[5] *Sector Outreach and Programs Division, Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington, DC 20598, USA. Enrique.Matheu@hq.dhs.gov*

ABSTRACT: The Common Risk Model for Dams (CRM-D), developed as a result of collaboration between the U.S. Army Corps of Engineers and the U.S. Department of Homeland Security, is a consistent, mathematically rigorous, and easy to implement methodology for security risk assessment of dams, navigation locks, hydropower projects, and similar infrastructures. The methodology provides a systematic approach for evaluating and comparing security risks across a large portfolio. Risk is calculated for an attack scenario (a specific adversary using a specific attack vector against a specific target) by combining consequence, vulnerability, and threat estimates in a way that properly accounts for the relationships among these variables. The CRM-D can effectively quantify the benefits of implementing a particular risk mitigation strategy and, consequently, enable return-on-investment analyses for multiple mitigation alternatives across a large portfolio. Recently, refinements have been made to the methodology to characterize the complexities of the adversary threat and the ability to interdict their actions. When first developed, CRM-D focused on a highly-capable international terrorist. Recently, it has been extended to include additional adversary types distinguished by a wide-range of capabilities. In addition, the methodology has been extended beyond target defenses to consider the role of local and national defenses in mitigating risk to manmade threats. A methodology for characterizing these defenses was developed as well as expert estimates for the probability an adversary could penetrate them. This comprehensive methodology provides a rigorous way to consider risks to dams across a large portfolio and is extensible to other types of critical infrastructures. This paper discusses various features of the CRM-D methodology as well as findings and lessons learned resulting from its implementation.

Keywords: Vulnerability, Threat, Conditional Risk, Portfolio Risk

1. INTRODUCTION

The Common Risk Model for Dams (CRM-D) methodology integrates outputs from three separate models: consequences, vulnerability, and threat. Modelling is a natural choice to estimate outcomes of complex physical and economic processes, such as consequences from attack, but it is equally important for estimating vulnerability and threat—variables that require more subjective input from subject matter experts (SME). It is prohibitively costly and time consuming to elicit expert judgments on vulnerability and threat for every scenario and to repeat the elicitation process every time a new scenario is introduced or old scenarios are modified. Therefore, modelling expert judgement is crucial when developing risk estimates to support return on investment (ROI) analyses, because the impact of potential risk mitigation alternatives needs to be assessed quickly.

The vulnerability and threat models are based on data elicited in a way that makes it possible to apply elicited SME judgment to any set of attack scenarios. The elicitations were conducted to estimate risk from an attack by a highly capable, transnational adversary groups. Elicitations in support of estimating risk from other types of adversaries are currently under development. Because the adversaries' capabilities and/or intent are likely to change with time, elicitations should be repeated every few years or as deemed appropriate.

2. CRM-D OVERVIEW

CRM-D incorporates commonly used risk metrics that are designed to be transparent, simple, and mathematically justifiable. The model also enables comparisons of calculated risks to assets and systems within and across critical infrastructure sectors.
The model/methodology take into account the unique features of dams and navigation locks and provide a systematic approach for evaluating and comparing risks from adaptive threats across a large portfolio.

At the most basic level of analysis, risk is estimated for an attack scenario, which is defined as (1) a specific adversary (e.g., a highly-capable transnational terrorist group), (2) attacking a specific target (e.g., the main impoundment structure of a specific dam), and (3) using a specific attack vector (e.g., a cargo van loaded with explosives). Risk is defined as *"expected of loss"*, which is a function of three variables: threat (T), vulnerability (V), and consequences (C):

$$R = f(T, V, C) \tag{1}$$

Threat is defined as the probability of an attack scenario being attempted by the adversary, given the attack on one of the targets in the portfolio under assessment, or P(A); vulnerability—as the probability of defeating the target's defenses, given that the attack is attempted, or P(S|A); and consequences—as the expected consequences of the attack, given that the target's defenses are defeated, C. Because of how CRM-D estimates these three variables, it is appropriate to calculate risk as their product:

$$R = P(A) \times P(S|A) \times C \tag{2}$$

[1]

CRM-D also defines "conditional risk," or R_C, as risk for the attack scenario, given that this scenario is chosen:[2]

$$R_C = P(S|A) \times C \tag{3}$$

The consequence and risk metrics currently considered in the CRM-D are loss of life and total economic impacts. The sum of all the risks for all the attack scenarios under consideration is termed *"portfolio risk."* Minimizing portfolio risk subject to available resources is often the focus of risk managers.

3. VULNERABILITY

CRM-D uses a layered defense model to evaluate the vulnerability of a target to a specific attack by a specific adversary. The defensive layers protecting a given target could potentially include national defenses (e.g., national counter-terrorism activities), local defenses (e.g., local law enforcement capabilities to detect and respond to potential attacks), and target defenses (e.g., onsite security systems and protective measures). The methodology for producing vulnerability estimates that account for target defensive layers is described in detail in Seda-Sanabria et al. (2011).

An attack is considered "successful" if every defensive layer is breached and the attack reaches the target. Therefore, for the conceptual attack scenario shown in Figure 1, P(S|A) can be determined using the following expression:

$$P(S|A) = P(S|A)_{L1} \times P(S|A)_{L2|L1} \times P(S|A)_{L3|L1,L2} \tag{4}$$

where $P(S|A)_{L1}$ is the probability of successfully breaching the first layer given the specific attacker under consideration attempts this attack, $P(S|A)_{L2|L1}$ is the conditional probability of successfully breaching the second layer given that the attacker has successfully breached the first layer, and $P(S|A)_{L3|L1,L2}$ is the conditional probability of successfully breaching the third layer given that the attacker has breached the first and the second layers.

[1] The functional relationships among the variables are accounted for by estimating P(A) as a function of the other two variables, but there is no stochastic relationship because P(S|A) and expected consequences are estimated as point values, and not random variables. This justifies the use of the product function (Cox, 2008).

[2] Note that the risk metric in Equation 2 is also conditional—on the attack within a portfolio under assessment. The "conditional risk" metric is further conditioned on the particular attack being chosen.

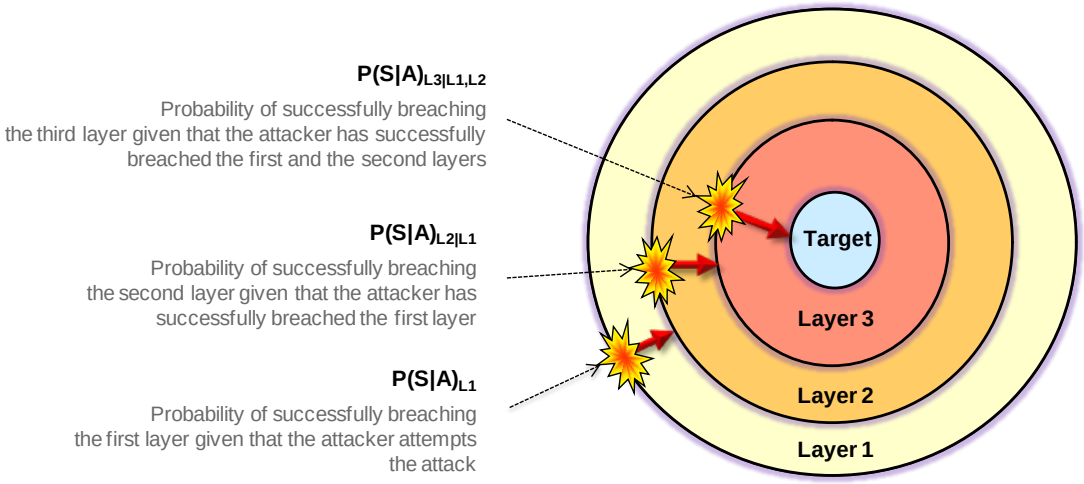

Fig. 1: Conceptual Model of Layered Defenses

Each layer is defined by its defensive attributes. For a national defensive layer, these can be the characteristics of relevant programs and activities implemented at the national scale, such as the security screening conducted at airports; for a local defensive layer, these can be the level of participation by local law enforcement agencies in intelligence information sharing and their prevention/response capabilities; and for the target defensive layers, these can be the characteristics of site security measures such as vehicle barriers, access control systems, security force, etc.

There are a relatively small number of combinations of defensive attributes that are typically implemented as target defensive layers at dams and related facilities. These commonly employed configurations are called layer defensive configurations, or LDCs. Because of the small number of LDCs, it is feasible to elicit probabilities of success for each reference attack vector against each LDC for each type of attacker under consideration. The vulnerability estimate for a given LDC reflects SME judgments about how well the defensive attributes of that LDC would perform against a particular attacker using a particular attack vector, based on the attacker's capabilities and intent and the attack vector's characteristics.

Probabilities of success against individual LDCs are combined into a P(S|A) for a scenario as shown in Equation 4. The probability of success against a layer is conditioned on which layers have already been breached, since some layers can degrade attackers' capabilities in various ways. Further, P(S|A) incorporates the possibility that some layers may or may not be encountered (e.g., response forces may or may not arrive in time to engage the adversary before the attack succeeds). The process for estimating P(S|A) in light of these factors is discussed in detail in Morgeson et al. (2013).

4. THREAT

Modelling threat from goal-oriented, adaptive adversaries is fundamentally different from modelling potential hazards associated with forces of nature. Adversaries *evaluate* potential attacks based on criteria that are important to them and then *choose* the attack that accords best with their objectives. When the adversary decision criteria change, their choice may change as well. Unlike consequence or vulnerability estimates, a threat estimate for an attack scenario depends not only on the characteristics of that scenario, but on the characteristics of all attack scenarios that the adversary is choosing from.

To account for these concepts, the CRM-D includes a *Probabilistic Adversary Decision Model* (PADM), which is composed of two sub-models: the *Adversary Value Model* (AVM) and the *Attack Choice Model* (ACM). The decision model is probabilistic because no aspect of the adversary's future decision process can be known with certainty.

4.1 Adversary Value Model

This model quantifies expert judgment about how adversaries evaluate the relative attractiveness of attack scenarios based on scenario characteristics that the adversary is likely to take into account. These features, related to the adversary capabilities and intent, reflect the various expected benefits, costs, and risks associated with each attack scenario. The AVM also quantifies the underlying uncertainty about the value system, which stems from the differences of opinion among experts and the uncertainty of each individual expert about the attacker value system.

4.2 Attack Choice Model

This model uses the estimated adversary value system to calculate P(A) for any set of attack scenarios and to perform ROI analyses for risk mitigation alternatives. To enable P(A) calculation, attack scenarios in the portfolio need to be formulated in terms that the AVM can accommodate. This involves using the CRM-D consequence and vulnerability models to estimate the values for loss of life, total economic impacts, and the probabilities of defeating the national/local and target defenses for every scenario in the portfolio. These variables are used as proxies for the adversary perceptions of these variables.

5. ADDED VALUE FOR THE POST 2015 FRAMEWORK FOR DISASTER RISK REDUCTION

The 2005 World Conference on Disaster Reduction (Hyogo, Japan), which gave rise to the "Hyogo Framework for Action 2005–2015", promoted a strategic and systemic approach to reducing vulnerabilities and risks to hazards—both natural and man-made. It established five priorities, four of which the CRM-D directly or indirectly addresses: (1) ensure that disaster risk reduction is a national and local priority with a strong institutional basis for implementation; (2) identify, assess and monitor disaster risks and enhance early warning; (3) use knowledge, innovation and education to build a culture of safety and resilience at all levels; and (4) reduce underlying risk factors. CRM-D accomplishes this by providing a framework that can be implemented locally at each dam to address security concerns, and nationally using the risk results from individual dams to conduct dam portfolio analyses. Furthermore, the CRM-D framework can be implemented across sectors. It provides the ability to monitor and assess risks and uses the information obtained to implement risk mitigation options that reduce the underlying risks. CRM-D also supports the Hyogo framework goal of creating and strengthening nationally integrated disaster risk reduction mechanisms among federated sectors or involving national systems that owned and operated by a diverse set of stakeholders.

6. CONCLUSIONS

The Common Risk Model for Dams (CRM-D) is a consistent, mathematically rigorous, and easy to implement method for security risk assessment of dams, navigation locks, hydropower projects, and similar infrastructures. This methodology, the implementation of which represents collaborative efforts between the U.S. Army Corps of Engineers and the U.S. Department of Homeland Security, provides a systematic approach for evaluating and comparing security risks across a large portfolio.

Risk is calculated for attack scenarios as a function of consequences, vulnerability, and threat. Vulnerability estimates are elicited as probabilities of successful attacks. The elicited estimates can then be used to estimate the vulnerability of a target protected by any combination of the generic security configurations against any of the reference attack vectors for the adversary groups under consideration. The CRM-D also incorporates a probabilistic adversary decision model to estimate the probability of each attack scenario in the set given that one of the scenarios in the set is attempted. The CRM-D can effectively quantify the benefits of implementing a particular risk mitigation strategy and, consequently, enable return-on-investment analyses for multiple risk mitigation alternatives across a large portfolio.

7. REFERENCES

Cox, Jr., Louis Anthony (Tony) (2008). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28, 1749–1761.

Dechant, Jason A. et al. (2012). The Common Risk Model for Dams: Methodology and Application, IDA Paper P-4761, Institute for Defense Analyses, Alexandria, VA.

Kirpichevsky, Yevgeniy et al. (2012). Estimating Threat from Adaptive Adversaries: Probabilistic Decision Modeling in the CRM-D, Draft Paper, Institute for Defense Analyses, Alexandria, VA.

Morgeson, J. Darrell; Seda-Sanabria, Yazmin; Matheu, Enrique E.; Keleher, Michael J. (2013). Incorporating Uncertainties in the Estimation of Vulnerabilities for Security Risk Assessments. *Proceedings 33rd U.S. Society of Dams Annual Meeting and Conference*, Phoenix, AZ.

Seda-Sanabria, Y., Fainberg, M. A., Matheu, E. E., Tressler, J. D., and Bowen, M. L. (2011). Implementation of the Common Risk Model for Dams for Security Assessments of USACE Critical Infrastructure. *Proceedings Dam Safety 2011 Conference*, Washington, DC.

United Nations (2007). *Hyogo Framework for Action 2005–2015: Building the Resilience of Nations and Communities to Disasters*, Geneva, Switzerland.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
June 2014	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NO.
A Consistent Approach for Security Risk Assessments of Dams and Related Critical Infrastructure	DASW01 04 C 0003
	5b. GRANT NO.
	5c. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)	5d. PROJECT NO.
J. Darrell Morgeson, Jason A. Dechant, Yevgeniy Kirpichevsky, Yazmin Seda-Sanabria, Enrique Matheu	5e. TASK NO. BA-6-3075
	5f. WORK UNIT NO.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NO.
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA NS Document D-5216

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM(S)
U.S. Army Corps of Engineers, Headquarters Office of Homeland Security 441 G Street NW (ATTN: CECW-HS) Washington, DC 20314	USACE, HQ
	11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Common Risk Model for Dams (CRM-D), developed in collaboration with the U.S. Army Corps of Engineers and the U.S. Department of Homeland Security, is a consistent, mathematically rigorous, and easy to implement methodology to assess the security risk at dams, navigation locks, hydropower projects, and similar infrastructures. It provides a systematic approach for evaluating and comparing security risks across a large portfolio. Risk is calculated for attack scenarios (a specific adversary using a specific attack vector against a specific target) by combining consequence, vulnerability, and threat estimates in a way that properly accounts for the relationships among these variables. The CRM-D can effectively quantify the benefits of implementing a particular risk mitigation strategy, enabling return-on-investment analyses for multiple mitigation alternatives across a large portfolio. Recently, refinements have been made to the methodology to characterize the complexities of adversarial threats and the ability to interdict their actions. In addition, this fully-featured methodology has been extended beyond site-specific defenses to consider the role of local and national defenses in mitigating the risk of attacks and is extensible to other types of critical infrastructures. This document discusses various features of the CRM-D methodology, as well as findings and lessons learned resulting from its recent implementation.

15. SUBJECT TERMS

Risk methodology, dams sector, critical infrastructure, vulnerability, threat, consequences

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jason A. Dechant
U	U	U	UU	4	19b. TELEPHONE NUMBER (Include Area Code) (703) 845-2495